قطب علمی رمز

انجمن رمز ایران

رمزگذاری جست‌وجو پذیر متقارن

اعظم سلیمانیان

دانشکده ریاضی– دانشگاه خوارزمی تهران

soleimani1985@gmail.com

چشم‌انداز

- ضرورت مسئله
- سناریو
  - رمزگذاری جست‌وجو پذیر متقارن
  - رمزنگاری جست‌وجوپذیر نامتقارن
- تاریخچه
- چند طرح معروف
  - طرح SSE2
  - طرح OXT
  - طرح OSPIR
- حملات
- جمع بندی

ضرورت مسئله

- سوال: روش مواجه با حجم وسیع اطلاعات و قدرت محاسباتی کم یا حافظه محدود چیست؟

  جواب: برون‌سپاری داده

- سوال: چطور داده‌های حساس را به یک سرور (کارگزار) نامعتمد بسپاریم؟

  جواب: رمزگذاری (حفظ محرمانگی داده)

- سوال: اگر هدف جست‌وجو روی داده‌های برون‌سپاری شده نزد سرور نامعتمد باشد چه باید کرد؟

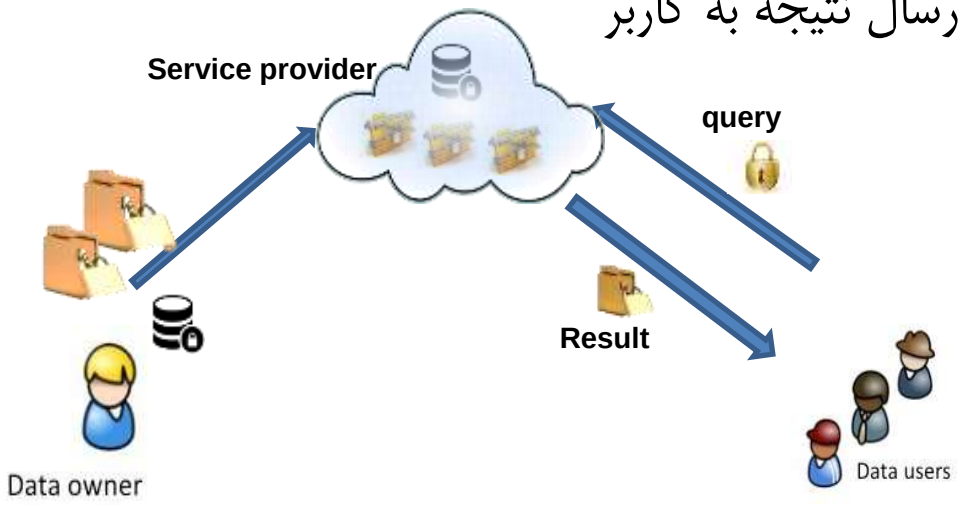
  جواب: بارگیری تمام داده‌ها، رمزگشایی و در نهایت جست‌وجو سمت کاربر

- فانتزی: جست‌وجو روی داده‌های رمز شده بدون نیاز به رمزگشایی

رمزگذاری جست‌وجوپذیر

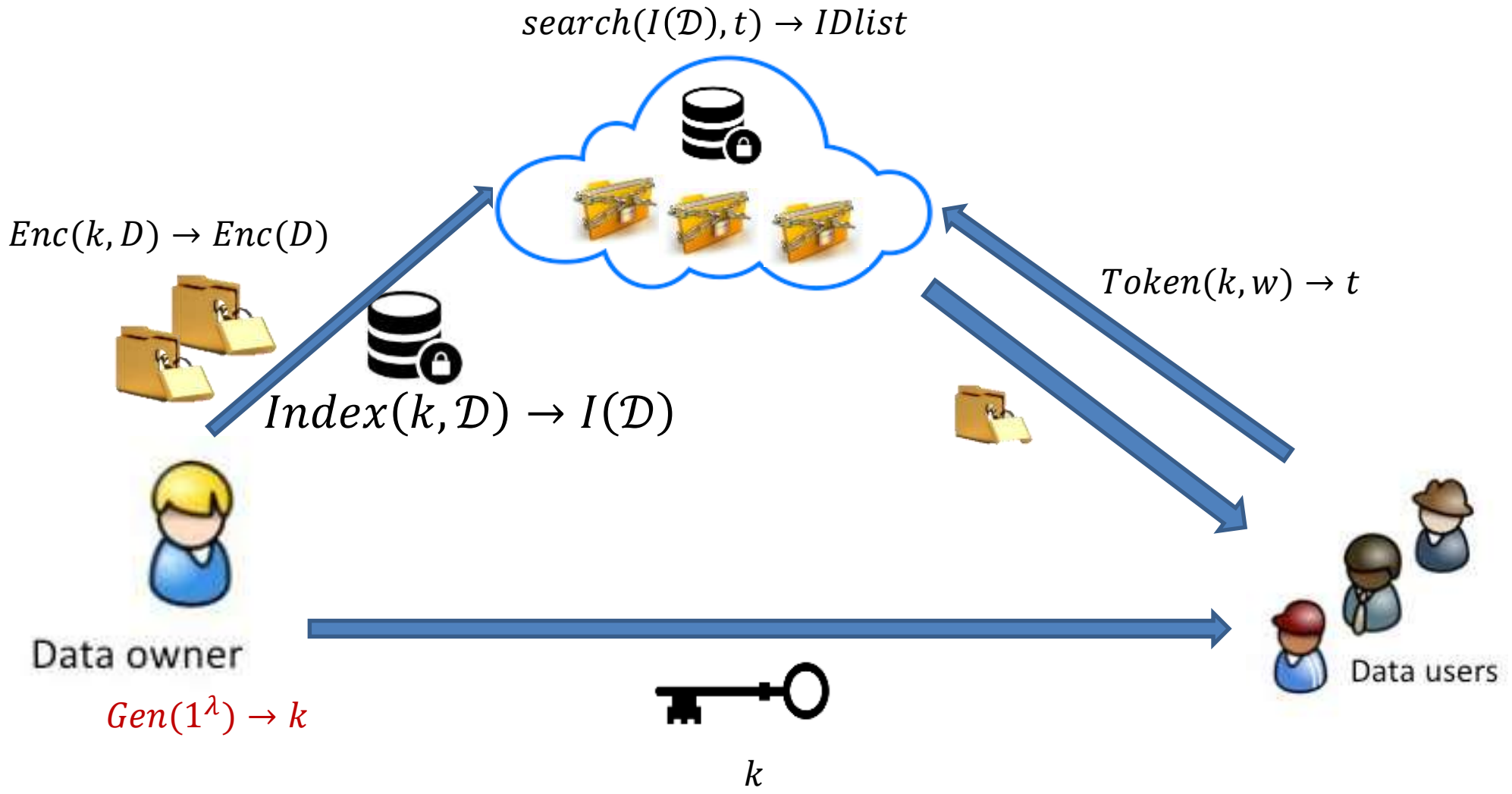
سناریو

- فاز برون‌سپاری:
  - کاربر(مالک داده): مجموعه‌ای از اسناد دارد، هر سند شامل یکسری لغت
  - مالک داده: رمزگذاری مجموعه اسناد و ساخت تعدادی داده ساختار
  - مالک داده: ارسال اسناد رمز شده و داده ساختارها به کارگزار
- فاز جست‌وجو:
  - کاربر: ارسال پرسمان رمز شده (نشان، Token) مبنی بر جست‌وجوی یک لغت خاص
  - کارگزار: پیدا کردن تمام اسناد شامل لغت مورد نظر و ارسال نتیجه به کاربر

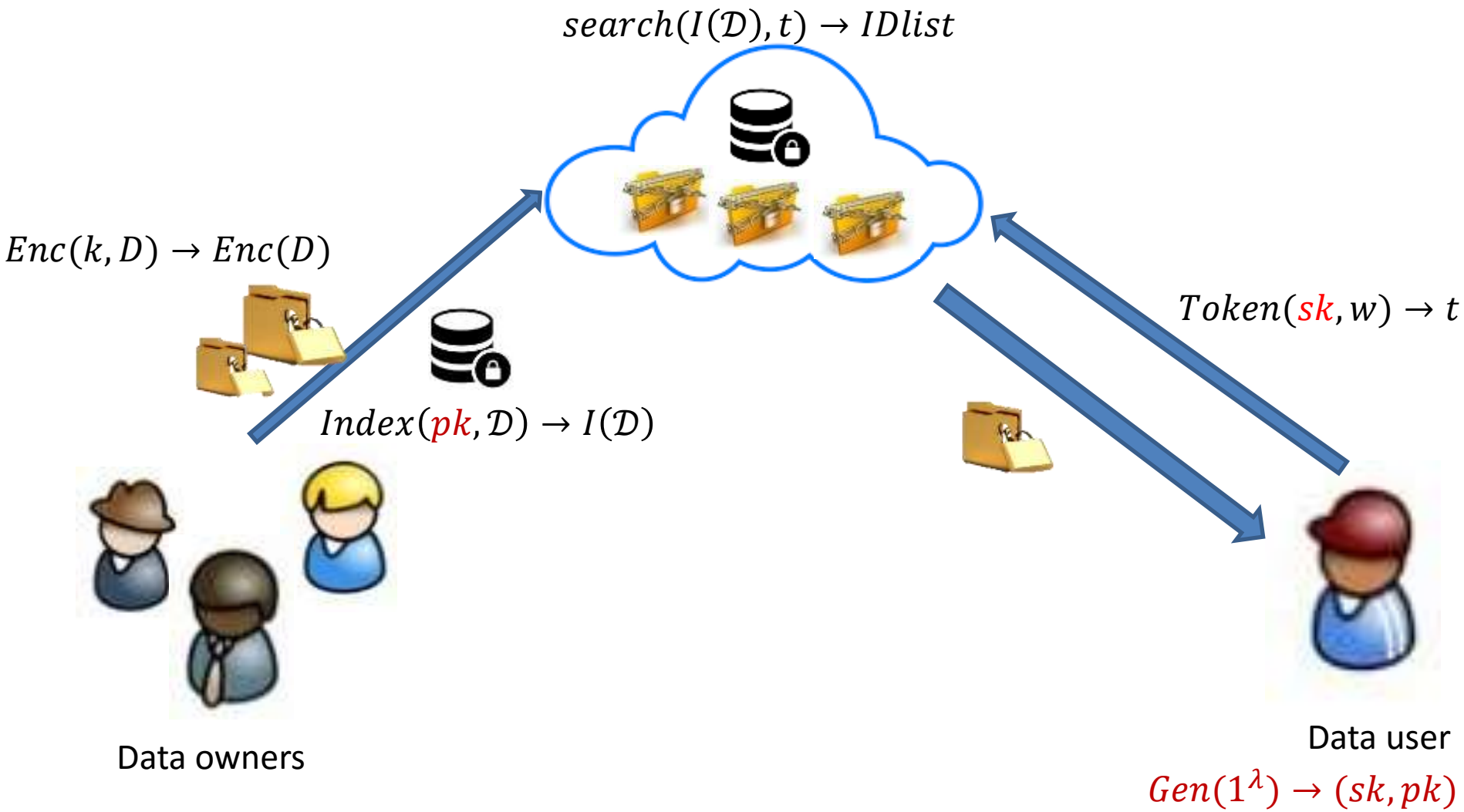


- امنیت
  - نشت الگوی دسترسی (شناسه اسناد خروجی)
  - نشت الگوی جست‌وجو (یکسان بودن پرسمان‌ها)
  - نشت اندازه مجموعه اسناد

رمزگذاری جستجوپذیر متقارن (SSE)



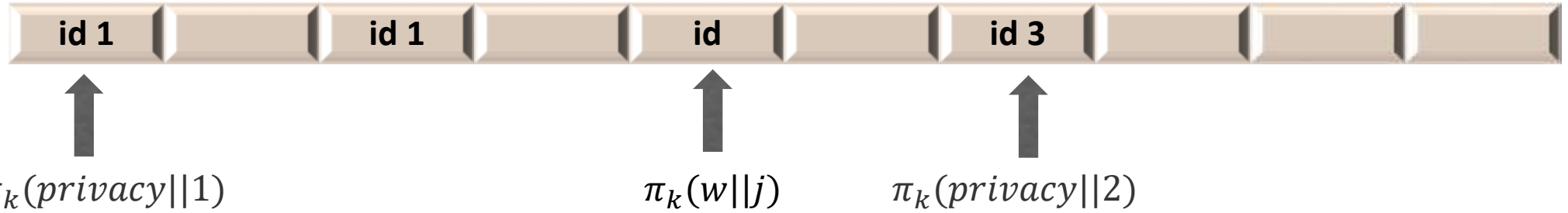
رمزگذاری جستجوپذیر نامتقارن(PEKS)



تاریخچه (SSE)

Scheme	Updates	Security	Search	Parallel	Queries
[SWP00]	No	CPA	O(|f|)	O(n/p)	SKS
[Goh03]	Yes	CKA1	O(n)	O(n/p)	SKS
[CM05]	No	CKA1	O(n)	O(n/p)	SKS
[CGKO06] #1	No	CKA1	O(OPT)	No	SKS
[CGKO06] #2	No	CKA2	O(OPT)	No	SKS
[CK10]	No	CKA2	O(OPT)	No	SKS
[vLSDHJ10]	Yes	CKA2	O(log m)	No	SKS
[KO12]	No	UC	O(n)	No	SKS
[KPR12]	Yes	CKA2	O(OPT)	No	SKS
[KP13]	Yes	CKA2	O(OPT·log(n))	$O(\frac{OPT}{p}\cdot\log(n))$	SKS
[CJJKRS13]	No	CKA2	O(OPT)*	No	Boolean
[HK14]	Yes	CKA2	O(n) | O(OPT)	No	SKS
[NPG14]	Yes	CKA2	O(OPT)	No	SKS
[CJJJKRS14]	Yes	CKA2	O(OPT)	Yes	SKS

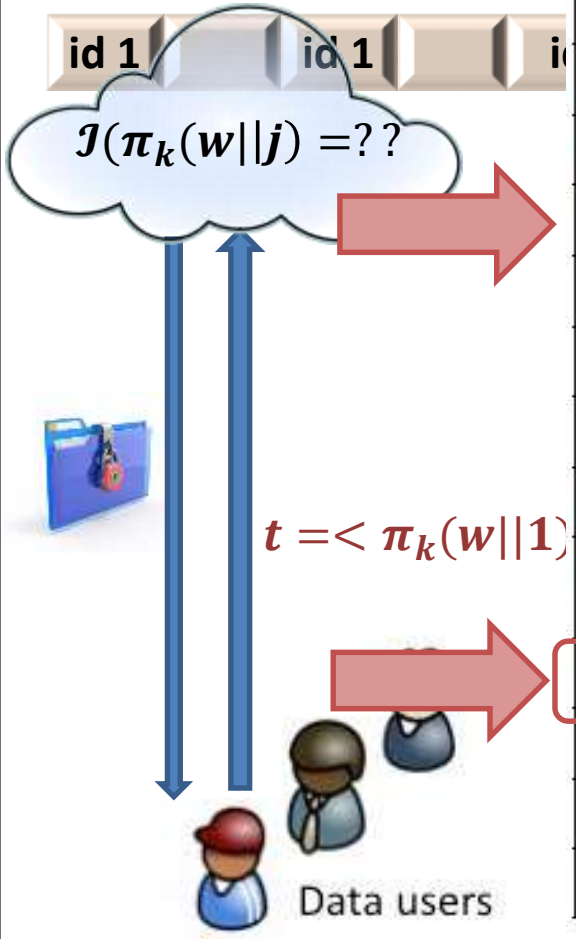
طرح SSE2 (Curtmola et al. 2006)



Index

searchable	id1, id2, id3
encryption	id1
homomorphic	id1, id2
privacy	id1, id3
cloud	id2, id3
query	id2, id3

طرح SSE2 (ادامه)



Scheme	Updates	Security	Search	Parallel	Queries
[SWP00]	No	CPA	O(|f|)	O(n/p)	SKS
[Goh03]	Yes	CKA1	O(n)	O(n/p)	SKS
[CM05]	No	CKA1	O(n)	O(n/p)	SKS
[CGKO06] #1	No	CKA1	O(OPT)	No	SKS
[CGKO06] #2	No	CKA2	O(OPT)	No	SKS
[CK10]	No	CKA2	O(OPT)	No	SKS
[vLSDHJ10]	Yes	CKA2	O(log m)	No	SKS
[KO12]	No	UC	O(n)	No	SKS
[KPR12]	Yes	CKA2	O(OPT)	No	SKS
[KP13]	Yes	CKA2	O(OPT·log(n))	$O(\frac{OPT}{p} \cdot \log(n))$	SKS
[CJJKRS13]	No	CKA2	O(OPT)*	No	Boolean
[HK14]	Yes	CKA2	O(n) | O(OPT)	No	SKS
[NPG14]	Yes	CKA2	O(OPT)	No	SKS
[CJJJKRS14]	Yes	CKA2	O(OPT)	Yes	SKS

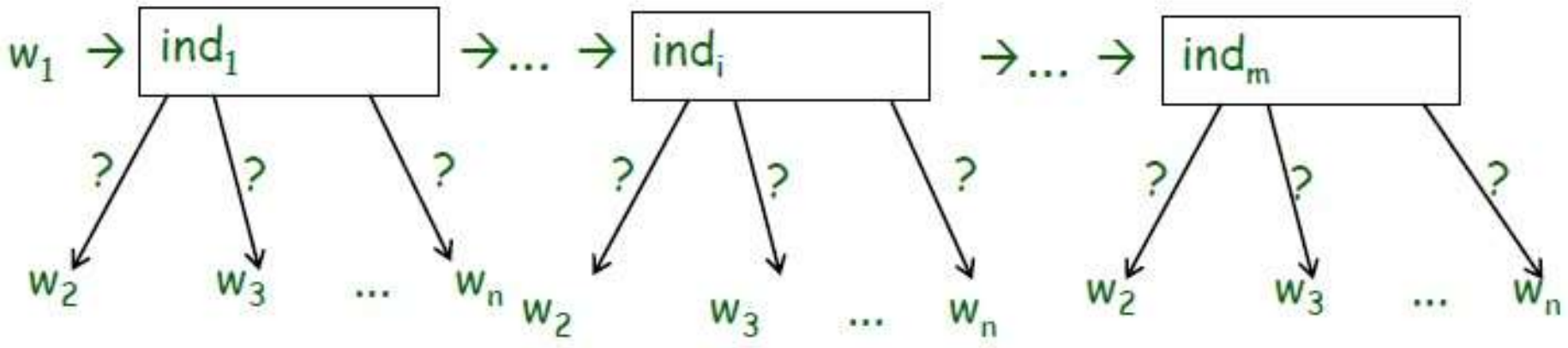
طرح OXT (Cash et al. CRYPTO13)

- ارایه یک طرح SKS کارا برای جستجوی تک لغت تنها با یک توکن.
- ارائه طرحی کارا برای جستجوی عبارتهای بولی $w_1 \wedge w_2 \wedge \cdots \wedge w_n$ (در حالت کلی $w_1 \wedge \varphi(w_2, \ldots, w_n)$)
- نیاز به تنها یک دور برای بازیابی اسناد متناظر با پرسمان بولی
- مدت زمان لازم برای پاسخ: قابل رقابت با پرسمان روی داده‌های آشکار
- مقاوم در برابر حمله ترکیب پرسمان
- نشت اطلاعات نسبتاً کم
- آزمایش شده روی مجموعه‌های بزرگ داده

- Enron email data set with more than 1.5 million documents
- DB consisting of 13 million documents (0.4TB of HTML files). Approximately one third of the latter database is a full snapshot of the English Wikipedia.

طرح OXT (ادامه)

- طرح در حالت آشکار، هدف جستجوی $w_1 \wedge w_2 \wedge \cdots \wedge w_n$
  - تعیین کلمه با کمترین فرکانس (مثلا w_1)
  - بازیابی اسناد شامل w_1 ← ساخت داده ساختاری ویژه SKS
  - برای هر یک از اسناد بازیابی شده، بررسی شامل شدن عبارت w_2 تا w_n ← ساخت داده ساختاری جهت بررسی عضویت



پروژه ESPADA/OXT

- IBM-UCI teams
- IARPA SPAR Program
  - David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner:Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries. CRYPTO (1) 2013: 353-373
  - Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner: Outsourced symmetric private information retrieval. ACM Conference on Computer and Communications Security 2013: 875-888
  - David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner: Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. IACR Cryptology ePrint Archive 2014: 853 (2014)
  - Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel-Catalin Rosu, Michael Steiner: Rich Queries on Encrypted Data: Beyond Exact Matches. ESORICS (2) 2015: 123-145

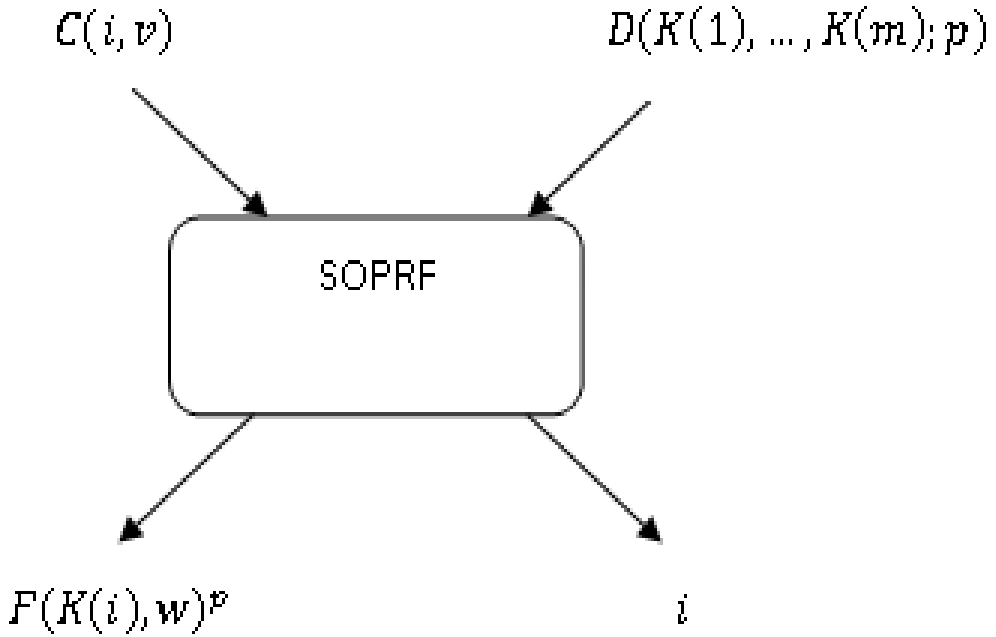
طرح OSPIR

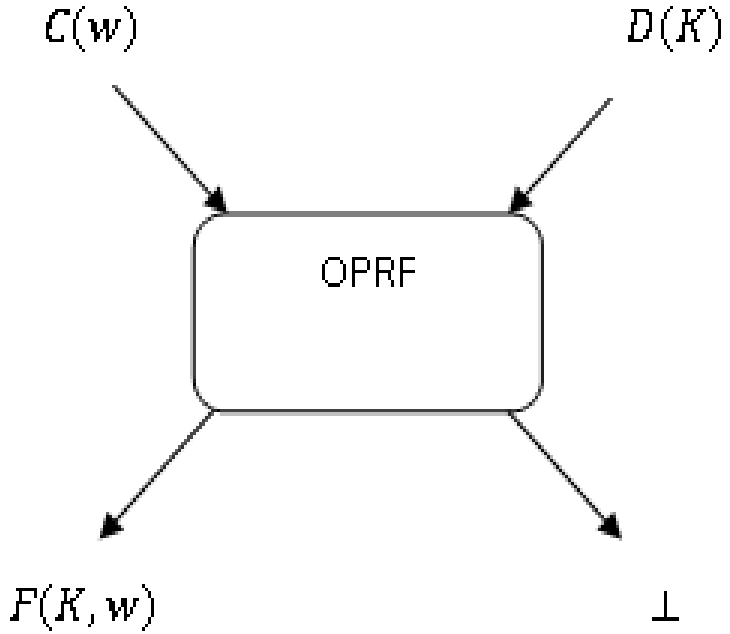
- توسعه طرح OXT به حالت چند کاربری (multi-client)
- اعمال کنترل دسترسی به صورت مجازشناسی کور(Blind Authorization)
- کنترل دسترسی در سطح پرسمان

- طرح اولیه:
  - کاربر به مالک داده: ارسال پرسمان $w_1 \wedge w_2 \wedge \cdots \wedge w_n$
  - مالک داده: بررسی سیاست دسترسی مختص کاربر
  - مالک داده: در صورت مجاز بودن کاربر،کمک به کاربر برای ساخت نشان (با همکاری کارگزار)
  - کاربر و کارگزار: اجرای طرح OXT

طرح OSPIR (Jarecki et al. 2013)

- مجوز دهی کور:
  - هر لغت به صورت زوج (مشخصه، مقدار)
  - کاربر به مالک داده: ارسال پرسمان $w_1 \wedge w_2 \wedge \cdots \wedge w_n$ بصورت بی‌تفاوت(oblivious)





حمله‌ها

- امنیت
  - نشت الگوی دسترسی (شناسه اسناد خروجی)
  - نشت الگوی جست‌وجو (یکسان بودن پرسمان‌ها)
  - نشت اندازه مجموعه اسناد

- حمله با استفاده از نشت الگوی دسترسی:

- Islam, M.S., M. Kuzu, M. Kantarcioglu, Access pattern disclosure on searchable encryption: Ramification, attack and mitigation, in: NDSS., vol. 20, pp. 1–12 (2012).
- Yupeng Zhang, Jonathan Katz, Charalampos Papamanthou: All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption. USENIX Security Symposium 2016: 707-720

- حمله با استفاده از نشت الگوی جست‌وجو:

- Liu, C., Zhu, L., Wang, M., Tan, Y.A., Search pattern leakage in searchable encryption: Attacks and new construction, Inform. Sci. 265, 176–188, (2014).

زمینه‌های تحقیقاتی

- جستجوی فازی (Fuzzy Keyword Search; Li et al. 2010)
- جستجوی رتبه بندی شده (Ranked Search; Cao et al. 2014)
- جستجوی پویا (Dynamic SE; Cash et al. 2013)
- جستجوی وارسی پذیر(Verifiable SE; Kurosawa et al. 2012)
- جستجوهای غنی (Rich Queries; Cash et al. 2013; Faber et al. 2015)
- جستجو روی داده‌های ساختار یافته(Structured SE; Kamara 2012)
- حمله‌ها (Attacks on SSE; Katz et al. 2016)

مراجع

- Reza Curtmola, Juan A. Garay, Seny Kamara, Rafail Ostrovsky: Searchable symmetric encryption: Improved definitions and efficient constructions. Journal of Computer Security 19(5): 895-934 (2011).
- David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner:Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries. CRYPTO (1) 2013: 353-373.
- Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner: Outsourced symmetric private information retrieval. ACM Conference on Computer and Communications Security 2013: 875-888
- David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, Michael Steiner: Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. IACR Cryptology ePrint Archive 2014: 853 (2014)

مراجع

- Sky Faber, Stanislaw Jarecki, Hugo Krawczyk, Quan Nguyen, Marcel-Catalin Rosu, Michael Steiner: Rich Queries on Encrypted Data: Beyond Exact Matches. ESORICS (2) 2015: 123-145
- Islam, M.S., M. Kuzu, M. Kantarcioglu, Access pattern disclosure on searchable encryption: Ramification, attack and mitigation, in: NDSS., vol. 20, pp. 1–12 (2012).
- Yupeng Zhang, Jonathan Katz, Charalampos Papamanthou: All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption. USENIX Security Symposium 2016: 707-720
- Liu, C., Zhu, L., Wang, M., Tan, Y.A., Search pattern leakage in searchable encryption: Attacks and new construction, Inform. Sci. 265, 176–188, (2014).

با تشکر از توجه شما